

# ABSTRACT OF THE DISCLOSURE

A multiple use ticket generating method is disclosed which enables a recipient to obtain signatures for arbitrarily many (correctly formed) messages after only one interaction with the  
 5 signer. The method provides a blind signature in a ticket, the signature having a multiple use with a built-in expiration. Then, the method develops a blinding value for the signature in a reproducible computation using a seed key substantially known only to the issuer of the ticket. The method implements a new class of signature schemes almost as efficiently as do previous one-time restrictive blind signature methods.

10

00401:024581US1